IN THE CLAIMS:

A listing of the status of all claims 1-24 in the present patent application is provided below.

1. (Previously Presented) A method for assembling fragmented network traffic, comprising:

detecting, by a monitoring node, an anomaly in the fragmented network traffic whereby two or more fragments within the fragmented network traffic have overlapping offsets;

performing a query to determine configuration information associated with how a destination node to which the two or more fragments are addressed is configured to reassemble overlapping fragments; and

reassembling the two or more fragments according to the configuration information associated with the destination node.

2. (Canceled)

3. (Previously Presented) The method as recited in claim 1 wherein determining that said two or more fragments have overlapping offsets comprises reading a header value associated with one of the fragments.

4. (Previously Presented) The method as recited in claim 3 wherein the header value comprises an offset value.

5. (Previously Presented) The method as recited in claim 1 wherein detecting an anomaly comprises determining that said two or more fragments overlap and that at least two of said fragments comprise different data for an overlapping portion of said fragments.

6. (Canceled)

7. (Previously Presented) The method as recited in claim 1 wherein performing a query includes querying the destination node.

8. (Previously Presented) The method as recited in claim 1 wherein performing a query includes querying an information base.

9. (Canceled)

10. (Previously Presented) The method as recited in claim 1 further including processing the anomaly to determine whether

the fragmented network traffic is associated with a threat.

11. (Previously Presented) The method as recited in claim 1 further including performing an action on the fragmented network traffic based on whether the fragmented network traffic is associated with a threat.

12. (Previously Presented) The method as recited in claim 1 further including discarding at least a portion of the fragmented network traffic if the fragmented network traffic is associated with a threat.

13. (Previously Presented) The method as recited in claim 1 further including copying one or more fragments comprising the fragmented network traffic to a buffer.

14. (Previously Presented) The method as recited in claim 1 further comprising sending an alert if an anomaly is detected.

15. (Previously Presented) The method as recited in claim 1 further comprising determining whether the fragmented network traffic should be blocked.

16. (Previously Presented) The method as recited in claim 1 further comprising determining whether the fragmented network traffic should be forwarded to the destination node.

17. (Canceled)

18. (Previously Presented) The method as recited in claim 1 further comprising determining that two or more fragments contained in said fragmented network traffic have overlapping portions.

19. (Previously Presented) The method as recited in claim 1 wherein detecting an anomaly comprises determining that two or more fragments contained in said fragmented network traffic have mismatching overlapping portions.

20. (Previously Presented) A system for assembling fragmented network traffic, comprising:

a memory configured to store at least a portion of the fragmented network traffic; and

a processor configured to:

detect an anomaly in the fragmented network traffic whereby two or more fragments within the fragmented network traffic have overlapping offsets;

perform a query to determine configuration information associated with how a destination node to which the two or more fragments are addressed is configured to reassemble overlapping fragments; and

reassemble the two or more fragments according to the configuration information associated with the destination node.

21. (Previously Presented) A computer readable storage medium comprising computer instructions for assembling fragmented network traffic, including instructions for:

detecting, by a monitoring node, an anomaly in the fragmented network traffic whereby two or more fragments within the fragmented network traffic have overlapping offsets;

performing a query to determine configuration information associated with how a destination node to which the two or more fragments are addressed is configured to reassemble overlapping fragments; and

reassembling the two or more fragments according to the configuration information associated with the destination node.

22. (Previously Presented) The system of claim 20 wherein performing a query includes querying the destination node.

23. (Previously Presented) The system of claim 20 wherein performing a query includes querying an information base.

24. (Previously Presented) The method of claim 1, further comprising initiating expanded buffering of fragments contained in said fragmented network traffic in response to detecting the anomaly.